UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/685,285	10/10/2000	John M. Hammer	05456.105008	4449

7590 08/11/2005

Steven P Wigmore Esq
King & Spalding
191 Peachtree Street NE
45th Floor
Atlanta, GA 30303

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 08/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/685,285	HAMMER ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9 and 11-65* is/are pending in the application.

4a) Of the above claim(s) *10* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9 and 11-65* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response of a Request for Continuation of Examination.

2. Claims 1-9 and 11-65 have been examined and are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-2, 4-9, and 11-65 are rejected under 35 U.S.C. 102(e) as being anticipated by Reps, et al. (US 6,070,190).

As per claim 1:

Reps, et al. disclose a method for automatically creating a record for one or more security incidents and reactions thereto, comprising the steps of:

recording computer security incident information with at least one of a date and time stamp **[see col.14, lines 1-21]**, the computer security incident information indicating one of suspicious computer activity that occurs prior to

a computer security threat and an actual computer security threat; **[see col.14, lines 55-57]**

classifying the computer security incident information; **[see col.11, lines 23-27 and col.25, lines 17-18 and 31-34]**

suggesting the procedure based on a classification of the computer security incident information; **[see col.11, lines 31-34 and col.25, lines 1-2 and 35-38]**

providing data to enable display of a procedure comprising one or more steps for one of investigating and responding to the computer security incident information; **[see col.11, lines 4-34 and col.19, lines 50-53]**

receiving a selection of one or more steps of a procedure; executing the selected one or more steps of the procedure; **[see col.15, lines 11-17]**

in response to executing the one or more steps of the selected procedure, recording executed procedure information and results of the executed procedure with at least one of a date and time stamp; and **[see col.14, lines 16-18]**

outputting a record comprising the computer security incident information, executed procedure information **[col. 25, lines 15-55]**, results of one or more steps of the executed procedure **[col.15, line 50-67]**, an identity of a user who selected the procedure **[see col.11, lines 63-65]**, and at least one of a corresponding date stamp and time stamp. **[see col.14, lines 16-18]**

As per claim 2: see col.9, lines 58-67; discussing an unmodifiable permanent database.

As per claim 4: see col.16, lines 33-37; discusses extracting the information from the results of an executed procedure.

As per claim 5: see col. 16, lines 38-57; discusses describing a computer security incident with said extraction information.

As per claim 6: see col.16, lines 57-65 and col.18, lines 28-30; discussing displaying information for a particular computer security incident to more than one user.

As per claim 7: see col.16, lines 19-32 and col.20, lines 25-36; discusses prepopulating fields of a record of a first program module from a second program module.

As per claim 8:

Reps discusses receiving security incident information from a first program module; processing the security incident information with a second program module; and forwarding the processed computer security incident information from the second program module to a third program module. **[col.24, lines 32-38 and col. 25, lines 15-55]**

As per claim 9: see col.13, lines 30-40; discusses receiving a selection of a procedure comprises automatically selecting a procedure with a program module.

As per claim 10: Cancelled

As per claim 11: see col.15, lines 11-15; discussing each steps are performed automatically by a program module.

As per claim 12: see col.15, lines 11-15; discussing some steps are performed automatically by a program module.

As per claim 13: see col.16, line 54-65 and col.20, lines 27-36; discusses displaying reports comprising one or more computer security incidents.

As per claim 14: see col.14, lines 40-45; discussing the results of an executed procedure comprise at least one of text, numbers, images, or formatted documents. **[the results must be in text, numbers, images, or formatted documents if a user can view it on the display]**

As per claim 15: see col.16, line 54-60; discusses predicting future actions of a source of a computer security incident.

As per claim 16: see col.16, lines 34-36; discusses identifying the source of a computer security incident.

As per claim 17: see col.14, lines 62-66; discusses sorting decoy or false security incidents from actual computer security incidents.

As per claim 18: see col.16, lines 54-60 and col.24, lines 32-38; discusses linking a first procedure to a second procedure.

As per claim 19: see col.10, lines 45-48; discusses determining the authorization level of a user.

As per claim 20: see col.11, lines 3-10 and col.18, lines 49-54; discusses providing data to enable display of a procedure further comprises the step of providing data for enabling display of one or more steps of a procedure.

As per claim 21:

Reps discusses providing data to enable display of a response procedure **[see col.11, lines 3-10]**; executing the response procedure **[col.14, lines 40-43]**; and in response to executing the response procedure, recording executed response procedure information and results of the executed response procedure with at least one of a date and time stamp. **[col.14, lines 44-52 and col. 25, lines 15-55]**

As per claim 22:

Reps discuss providing data to enable display of an investigation procedure; executing the response procedure; and **[col.19, lines 27-39 and col.21, lines 27-56]** in response to executing an investigation procedure **[col.19, lines 40-61]**, recording executed response procedure information and results of the executed response procedure with at least one of a date and time stamp. **[col.14, lines 3-21]**

As per claim 23: see col.11, lines 3-10; discusses providing data to enable display of a procedure further comprises the step of providing data to enable display of one or more steps of the response procedure.

As per claim 24: see col.14, lines 40-43; discusses providing data to enable display of results of the executed procedure.

As per claim 25: see col.19, lines 54-61; discusses providing data to enable display of results of the executed procedure.

As per claim 26: see col.20, lines 25-31; discusses identifying an appropriate computer to execute a step in the investigation procedure; and identifying an appropriate computer to execute a step in the response procedure.

As per claim 27:

Reps discusses accessing a table comprising computer locations and step information **[col.5, lines 46-48 and col.11, lines 48-52]**; comparing a step to be executed with computer locations listed in the table; determining if a match exists between the step to be executed and the computer locations **[col.14, lines 62-66 and col.25, lines 31-38]**; and if one or more matches exist, displaying the matching information or automatically selecting appropriate location. **[col.23, lines 27-48 and col.25, lines 39-42]**

As per claim 28: see col.11, lines 50-52 and col.25, lines 31-37; discussing the table further comprises Internet address ranges, the method further comprising the step of comparing an Internet address of a source of a computer security incident with the Internet address ranges of the table.

As per claim 29: see col.9, lines 24-35; discusses providing data to enable display of an appropriate substitute computer location if a match does not exist.

As per claim 30: see col.16, lines 34-67; discusses identifying an appropriate computer to execute a step in either an investigation or a response procedure,

wherein the computer is strategically located relative to a source of a security incident.

As per claim 31: see col.13, lines 30-40; discusses executing one or more program modules in response to a selection of a procedure.

As per claim 32: see col.9, lines 24-35 and col.17, lines 45-67; discussing one or more program modules comprises one or more software application programs that can operate as a stand alone programs.

As per claim 33: see col.15, lines 7-10 and col.17, lines 45-67; discussing one or more program modules comprises an off the shelf software application programs.

As per claim 34: see col.14, lines 62-66; discussing the security incident information comprises predefined attributes.

As per claim 35:

Rep discussing the predefined attributes **[col. 25, lines 15-55]** comprise any one of a computer incident severity level, a computer incident category, a computer incident scope value, a computer incident status value, an attacker internet protocol (IP) address value, an attacker ISP name, an attacker country, an external attacker status value, an incident type value, a vulnerabilities level, an entry point value, an attack profile value, a target networks value, a target firewalls value, a target hosts value, a target services value, a target accounts value, and a damage type value. **[col.11, lines 15-26 and col.12, lines 1-3]**

As per claim 36: see col.11, lines 15-26; discussing the security incident information comprises attributes that are at least one of variable and computer-generated.

As per claim 37: see col.11, lines 15-26; discusses whether a computer security incident comprises an actual breach in security based upon values of its attributes.

As per claim 38: see col.11, lines 28-34; discusses receiving a selection for a step of a procedure; and generating a pre-execution warning prior to the selection of a step.

As per claim 39:

Rep discusses receiving a selection for a step of a procedure, executing the selected step **[see col.15, lines 11-17]**, and suggesting an appropriate subsequent step in the procedure. **[col.15, lines 20-41]**

As per claim 40: see col.13, lines 30-40 and col.15, lines 11-15; discussing each step is performed automatically in response to a detected computer security incident.

As per claim 41:

Reps discusses providing data to enable display of a plurality of computer tools in a non-procedural manner; receiving a selected for a computer tool **[col.9, lines 24-35 and lines 55-57]**; and executing the selected computer tool. **[col.15, lines 7-15]**

As per claim 42:

Reps, et al. disclose a method for organizing and recording reactions to one or more security incidents, comprising the steps of:

classifying the computer security incident information; **[see col.11, lines 23-27 and col.25, lines 17-18 and 31-34]**

suggesting the procedure based on a classification of the computer security incident information; **[see col.11, lines 31-34 and col.25, lines 1-2 and 35-38]**

providing data to enable display of one or more computer security investigation procedures for investigating **[see col.11, lines 4-34]** one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security threat; **[see col.14, lines 55-57 and col.19, lines 50-53]**

providing data to enable display of the one or more security response procedures comprising one or more steps for one of investigating and responding to the computer security incident information; **[see col.19, lines 4-43-62]**

in response to a selection of a computer security investigation procedure, providing data to enable display of one or more corresponding investigation steps; **[col.19, lines 40-61]**,

in response to a selection of a computer security response procedure, providing data to enable display of one or more corresponding response steps; and **[col.14, lines 44-52]**

generating a permanent record comprising security incident information, executed investigation step and result information **[col. 25, lines 15-55]**, executed response step and result information, and corresponding date and time stamps. **[see col.14, lines 1-21]**

As per claim 43: see col.14, lines 3-18 and col.19, lines 41-54; discussing recording executed investigation step information and results of the executed investigation step with at least one of a date and time stamp in response to a selection of a step of a response procedure.

As per claim 44: see col.14, lines 3-43; discussing recording executed response step information and results of the executed response step with at least one of a date and time stamp in response to a selection of a step of a response procedure.

As per claim 45:

Reps discuss providing data to enable display of a plurality of procedures;

in response to receiving a selection of a procedure, displaying a plurality of steps **[col.14, lines 3-43]**; obtaining modification information for the selected procedure; and storing the modification information. **[col.20, lines 27-25-45 and col.25, lines 31-53]**

As per claim 46: see col.25, lines 31-53; discusses adding or deleting a step in a procedure.

As per claim 47:

Reps discusses providing data to enable display of a plurality of steps of a procedure **[see col.11, lines 1-10 and lines 42-47]**; in response to receiving a selection of a step, providing data to enable display of detailed information fields related to the selected step **[see col.19, lines 27-39]**; obtaining modification information for the selected step; and storing the modification information. **[col.20, lines 27-25-45 and col.25, lines 31-53]**

As per claim 48: see col.20, lines 27-25-45 and col.25, lines 31-53; discusses adding, deleting or modifying a step in a procedure.

As per claim 49:

Reps discusses obtaining computer security incident search information and providing data to enable display of a plurality of one or more computer security incidents matching the computer security incident search information. **[col.16, lines 34-65]**

As per claim 50:

Reps discuss tracking multiple computer security incidents and storing information for each computer security in accordance with at least one of date and time stamp. **[col.14, lines 3-43]**

As per claim 51:

Reps discloses a method for selecting a computer that is strategically located relative to a source of a security incident, comprising the steps of:

accessing a table comprising computer, Internet address ranges associated with the computer locations **[see col.5, lines 46-48 and col.11, lines 51-52]**, and computer security step information associated with the computer locations, the computer security step information for one of investigating **[see col.17, lines 60-67 and col.23, lines 28-35]** one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security threat **[see col.10, lines 21-26 and col.11, lines 28-34]**, the computer location identifying devices that are able to perform the computer security step information; **[see col.24, lines 48-66]**

comparing a computer security step to be executed and a target Internet address with computer locations and Internet address ranges listed in the table; **[col.14, lines 25-66 and col. 25, lines 15-32]**

determining if a match exists between the computer security step to be executed and the computer locations; **[col.23, lines 27-48 and col.25, lines 39-42]**

determining if a match exists between an Internet address of a computer security incident and Internet address ranges listed in the table; and **[col.25, lines 31-37]**

selecting a computer to execute the computer security step based upon the matching steps, wherein the computer has a location and is capable of interacting with the Internet address of the security incident. **[col.11, lines 23-65 and col.25, lines 39-43]**

As per claim 52:

Reps discusses if one or more matches exist, providing data to enable display of the matching information and if a match does not exist, providing data to enable display of one or more appropriate substitute computer location or automatically selecting an appropriate location. **[col.9, lines 24-35]**

As per claim 53: see col.16, lines 34-67; discusses a portion of a computer security response procedure, wherein the computer is strategically located relative to a source of a security incident.

As per claim 54: see col.19, lines 27-46; discusses a portion of a computer security investigation procedure, wherein the computer is strategically located relative to a source of a security incident.

As per claim 55: see col.15, lines 7-10; discussing one or more off the shelf security application programs.

As per claim 56:

Reps discloses a method for generating a permanent record or one or more computer security incidents and reactions thereto, comprising the steps of:

receiving the computer security incident information **[col. 25, lines 5-16]** indicating one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security threat; **[see col.14, lines 55-57]**

classifying the computer security incident information; **[see col.11, lines 23-27 and col.25, lines 17-18 and 31-34]**

displaying one or more tools **[col.9, lines 55-57 and col.19, lines 51-53]** for one of investigating **[see col.11, lines 4-34]** one of suspicious computer activity that occurs prior to a computer security threat and an actual computer security threat; **[see col.14, lines 55-57]**

suggesting a tool based on a classification of the computer security incident information; **[see col.11, lines 31-34 and col.25, lines 1-2 and 35-38]**

receiving a selection of a tool; **[col.15, lines 7-15]**

in response to a selection of a tool, forwarding data for execution of the tool; and **[col.13, lines 17-25 and col.19, lines 41-46]**

forwarding data for generating a permanent record comprising computer security incident information, executed tool information, and corresponding date and time stamp. **[col.14, lines 3-43]**

As per claim 57: see col.11, lines 3-6; discusses displaying the tools as icons on a computer display.

As per claim 58: see col.12, lines 1-10 and lines 17-23; discusses displaying a plurality of tools that are selectable from a menu.

As per claim 59: see col.12, lines 17-23 and col.17, lines 45-67; discusses installing the one or more program modules within a single program on a server.

As per claim 60: see col.9, lines 25-28 and col.12, lines 17-23; discusses installing the one or more program modules on a single server.

As per claim 61: see col.17, lines 45-67; discusses installing the one or more program modules on a computer that is a target of a computer incident.

As per claim 62: see col.9, lines 52-57; discusses installing the one or more program modules on both a computer that is a target of a computer incident and a server.

As per claim 63: see col.14, lines 62-66 and col.17, lines 18-28; discussing comparing an Internet address of a computer subject to an attack or a security breach with the Internet address ranges of the table.

As per claim 64: see col.14, lines 62-66 and col.25, lines 31-50; discussing comparing an Internet address of a witness to a computer security incident with the Internet address ranges of the table.

As per claim 65: see col.17, lines 18-28 and col.25, lines 31-50; discussing comparing an Internet address of an accomplice to a computer security incident with the Internet address ranges of the table.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claim 3 are rejected under 35 U.S.C. 103(a) as being obvious over Reps, et al. (US 6,477,585) and further in view of Todd Sundsted.

As per claim 3:

Reps disclose recording security incident information with at least one of a date and time stamp **[see col.10, lines 28-56 and col.14, lines 10-40]** and providing data to enable display of a procedure **[see col.11, lines 1-10 and lines 42-47]**. The time signature is a form of computer security incident information that tells the time and date file or a message, which is a time/date stamp of a file/message (i.e. when created, the last modification, or when received or sent). However, Reps fails to include the teachings of a digital signature.

Sundsted teaches a digital signature that is generated from a file/message and comes with a secret key. Sundsted teaches the digital signature cannot be forged that would not change the file/message without invalidating the signature, which means the integrity of the message is kept by having a digital signature.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include a digital signature of Sundsted with the teachings of Reps would be to maintain the authenticity and integrity of the file/message.

Response to Arguments

4. Applicant's arguments with respect to claims 1-9 and 11-65 have been considered but are moot in view of the new ground(s) of rejection.

The Examiner finds the claim language to be broad even after the newly amended claims. Hence, the Examiner gives the broadest reasonable interpretation for what is claimed.

The computer security incident information is broad leaving this limitation open for anything that can be considered as a security incident for a computer. A computer security incident can read literally as a violation to the computer (col.11, line 32) the terminology does not identify what is considered a computer security incident or the type of violation. For security incidents, the Examiner can interpret it as anything related to security of a computer or system such as a possible threat, a certain known threat, an unsuccessful service response, an unavailable computer occurrence, or a violation. Hence, a computer security incident information in Reps is a computer violation (col.25,

line 34), a server computer that was recorded as not available (col.10, lines 40-41) or unsuccessful service response (col.15, lines 40-41).

Reps, et al. does teach recording the computer incident information (col.5, lines 24-26 and col.10, lines 40-41) with at least a date and time stamp (col.14, lines 14-16) wherein the computer security incident indicates one of suspicious computer activity (col.10, lines 22-26) such as a violation that occurs prior to a computer security threat and an actual threat (col.14, lines 63-66 and col.15, lines 19-46).

Further, the new limitations of classifying the computer security incident information and suggesting the procedure base on the classification of the computer security incident information is also broad because these limitations does not express what type of security incident being classified or how it was classified. So this leaves it open to merely classifying any security incident that occurred prior to the computer security threat or is occurring and can read on just having the type of violations that have been recorded or is occurring. Therefore, Reps does teach the new limitations of classifying the computer security incident information (col.19, line 60 – col.20, line 6) by the type of violation that have been recorded (col.25, line 18) such as statistical performance of each server to determine which server(s) exhibited poor response time on the day in question or server location violation type (col.25, line 34) and suggesting the procedure by having problem determination process wherein Reps includes having remediation steps and how to inform the

violation based on the type of violation of the computer(s) (col.11, lines 33-34 and col.25, lines 1-2 and 35-38).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100